

**Exam : Cisco 642-545**

**Title : Implementing Cisco  
Security Monitoring,  
Analysis and Response  
System**

**Version : Demo**

## Important Note, Please Read Carefully

### Other VisualExams products

[All visual exams IT Exam Products](#)

### Our products of Offline Testing Engine

Use the offline Testing engine product to practice the questions in an exam environment.

Build a foundation of knowledge which will be useful also after passing the exam.

[visual exams Testing Engine](#)

### Latest Version

We are constantly reviewing our products. New material is added and old material is revised. Free updates are available for 90 days after the purchase. You should check your member zone at VisualExams and update 3-4 days before the scheduled exam date.

Here is the procedure to get the latest version:

1. Go to <http://www.visual exams.com/>
2. Log in the **User Center**
3. The latest versions of all purchased products are downloadable from here. Just click the links.

### Feedback

If you spot a possible improvement then please let us know. We always interested in improving product quality.

Feedback should be send to [Visual exams@hotmail.com](mailto:Visual exams@hotmail.com). You should include the following: Exam number, version, page number, question number, and your login Account.

Our experts will answer your mail promptly.

### Explanations

This product does not include explanations at the moment. If you are interested in providing explanations for this exam, please contact [Visual exams@hotmail.com](mailto:Visual exams@hotmail.com).

### Features

- Comprehensive questions with complete details
- Instant Downloadable in PDF form.
- Verified Answers Researched by Industry Experts
- Questions accompanied by exhibits.
- Drag and Drop questions as experienced in the Actual Exams.
- These questions and answers are backed by our GUARANTEE.
- Questions updated on regular basis.
- Like actual certification exams our product is in multiple-choice questions (MCQs)

**Commitment to Your Success: At VisualTestExam.com, we are committed to your ongoing success. Our exams and questions are constantly being updated and compared to industry standards.**

Want to earn a Microsoft certification like MCSE, MCSE 2003, CCNA, CCNP? Thinking about getting an A+ or CCSP?

A, CCSP or Network+ Certification with less effort and time. You will be astonished at the theoretical and practical knowledge you will acquire in such a short period of time using our Certification Training Products. Our Study material will enable you to pass your Microsoft, Your Cisco and any other certification on the very first attempt.

## **Guarantee**

Visualexams provides the most competitive quality of all exams for the customers, we guarantee your success at the first attempt with only our Certification Question&Answers, if somehow you do not pass the exam at the first time, we will not only arrange FULL REFUND for you, but also provide you another exam of your claim, ABSOLUTELY FREE!

1. Which attack can be detected by Cisco Security MARS using NetFlow data?

- A. man-in-the middle attack
- B. day-zero attack
- C. spoof attack
- D. Land attack
- E. buffer overflow attack

**Answer: B**

2. What is used to publish events to Cisco Security MARS about Cisco IPS signatures that have fired?

- A. SNMP
- B. SSL
- C. HTTPS
- D. SDEE
- E. syslog
- F. Secure FTP

**Answer: D**

3. Which statement best describes the case management feature of Cisco Security MARS?

- A. It is used to automatically collect and save information on incidents, sessions, queries, and reports dynamically without user interventions.
- B. It is used to capture, combine, and preserve user-selected Cisco Security MARS data within a specialized report.
- C. It is used to very quickly evaluate the state of the network.
- D. It is used in conjunction with the Cisco Security MARS incident escalation feature for incident reporting.

**Answer: B**

4. Which statement is true about the case management feature of Cisco Security MARS?

- A. Cases are created on a global controller, but they can be viewed and modified on a local controller.
- B. The global controller has a Case bar and all cases are selected from the Query/Reports > Cases page.
- C. Cases are created on a local controller, but they can be viewed and modified on a global controller.

D. The Cases page on a local controller has an additional drop-down filter to display cases per a global controller.

**Answer: C**

5. At what level of operation does the Cisco Security MARS appliance perform NAT and PAT resolution?

- A. Local (Level 0)
- B. Basic (Level 1)
- C. Intermediate (Level 2)
- D. Advanced (Level 3)
- E. Global (Level 4)

**Answer: C**

6. Which three statements are true about Cisco Security MARS rules? (Choose three.)

- A. There are three types of rules.
- B. Rules can be saved as reports.
- C. Rules can be deleted.
- D. Rules trigger incidents.
- E. Rules can be defined using a seed file.
- F. Rules can be created using a query.

**Answer: ADF**

7. Which action enables the Cisco Security MARS appliance to ignore false-positive events by either dropping the events completely, or by just logging them to the database?

- A. creating system inspection rules using the drop operation
- B. creating drop rules
- C. inactivating the rules
- D. inactivating the events
- E. deleting the false-positive events from the Incidents page
- F. deleting the false-positive events from the Event Management page

**Answer: B**

8. Which two configuration options enable the Cisco Security MARS appliance to perform mitigation?

(Choose two.)

- A. SNMP RW community string
- B. Cisco Security MARS integration with Cisco Security Manager
- C. Telnet or SSH access type with SNMP RO community
- D. a NetFlow device added in the Cisco Security MARS database
- E. SSL communications with the network devices

**Answer: AC**

9. What is a supported mitigation feature on the Cisco Security MARS appliance?

- A. generating and pushing configuration commands to Layer 3 devices
- B. generating and pushing configuration commands to Layer 2 devices
- C. automatically dropping all suspected traffic at the nearest IPS appliance
- D. storing and identifying NetFlow data for attack mitigation

**Answer: B**

10. What are the two options for handling false-positive events reported by the Cisco Security MARS appliance? (Choose two.)

- A. archive to NFS only
- B. save as a false-positive report
- C. drop
- D. mitigate at Layer 2
- E. log to the database only
- F. escalate to the Cisco Security MARS administrator

**Answer: CE**

Visualexams.com was founded in 2006. The safer,easier way to help you pass any IT Certification exams . We provide high quality IT Certification exams practice questions and answers(Q&A). Especially Adobe, Apple, Citrix, Comptia, EMC, HP, HuaWei, LPI, Nortel, Oracle, SUN, Vmware and so on. And help you pass any IT Certification exams at the first try.

Web site: <http://www.visualexams.com>

You can reach us at any of the email addresses listed below.

E-Mail: [visualexams \(at\) hotmail.Com](mailto:visualexams@hotmail.com)